Presented at the 1989 IEEE Conference on Decision and Control

September 1989

LIDS-P-1912

OUTPUT STABILIZABILITY OF DISCRETE EVENT DYNAMIC SYSTEMS

C. M. Özveren, A. S. Willsky
Dept. of Electrical Engineering and Computer Science
Lab. for Information and Decision Systems
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139

1 Introduction

The study of the control of Discrete Event Dynamic Systems (DEDS) has been introduced by Wonham, Ramadge, et al. [2,7,8,10]. This work has prompted a considerable response by other researchers, exploring a variety of alternate formulations and paradigms. In our work, we have had in mind the development of a regulator theory for DEDS. In another paper, [4], we develop notions of stability and stabilizability for DEDS while in [3], we focus on the questions of observability and state reconstruction,using what might be thought of as an intermittent observation model. In this paper, we combine our work on stabilizability and observability to address the problem of stabilization by dynamic output feedback under partial observations. Our presentation here is necessarily brief, and we refer to [5] for details.

2 Background and Preliminaries

The class of systems we consider are defined over $G = (X, \Sigma, \Gamma, U)$, where X is the finite set of states, with $n = |X|$, Σ is the finite set of possible events, $\Gamma \subset \Sigma$ is the set of observable events, and U is the set of admissible control inputs consisting of a specified collection of subsets of Σ, corresponding to the choices of sets of controllable events that can be enabled. The dynamics defined on G are:

$$x[k+1] \in f(x[k], \sigma[k+1]) \quad (2.1)$$

$$\sigma[k+1] \in (d(x[k]) \cap u[k]) \cup e(x[k]) \quad (2.2)$$

The function d specifies the set of possible events defined at each state,$e(x)$ specifies the subset of $d(x)$ events that *cannot* be disabled at each state, and the function f specifies the nondeterministic state evolution. In Section 4, we use this general framework in which there is no loss of generality in taking $U = 2^{\Sigma}$. Up to that point we assume the slightly more restrictive framework of [8] in which $U = 2^{\Phi}$ and $e(x) = d(x[k]) \cap \overline{\Phi}$ Furthermore, we assume that $\Phi \subset \Gamma$.

Our model of the output process is quite simple: whenever an event in Γ occurs, we observe it; otherwise, we see nothing. Specifically, with $h(\sigma) = \sigma$ if $\sigma \in \Gamma$ and $h(\sigma) = \epsilon$ otherwise, where ϵ is the "null transition", our output equation is

$$\gamma[k+1] = h(\sigma[k+1]) \quad (2.3)$$

Note that by letting $h(s_1, s_2) = h(s_1)h(s_2)$ we can think of h as a map from Σ^* to Γ^*, where Γ^* denotes the set of all strings of finite length with elements in Γ, including the empty string ϵ. The quadruple $A = (G, f, d, h)$ represents our system.

Throughout this paper we will assume that A is *alive*, i.e. $\forall x \in X$, $d(x) \neq \emptyset$. Another notion that we need is the composition of two automata, $A_i = (G_i, f_i, d_i, h_i)$ which share some common events. The dynamics of the composition are specified by allowing each automaton to operate as it would in isolation except that when a shared event occurs, it *must* occur in both systems [5]. We also need:

Definition 2.1 *Let E be a subset of X. A state x is* E-pre-stable *if there exists some integer i such that every trajectory from x passes through E in at most i transitions. The state x is* E-stable *if every state reachable from x is E-pre-stable. The DEDS is* E-stable *(respectively,* E-pre-stable*) if every x is E-stable (E-pre-stable).* •

Definition 2.2 *The* radius *of A is the length of the longest cycle-free trajectory between any two states of A. The* E-radius *of an E-stable system A is the maximum number of transitions it takes any trajectory to enter E.* •

We refer the reader to [4] for a more complete discussion of this subject and for an $O(n^2)$ test for E-stability of a DEDS. In [4] we also study stabilization by state feedback. Here, a state feedback law is a map $K : X \rightarrow U$ and the resulting closed-loop system is $A_K = (G, f, d_K, h)$ where

$$d_K(x) = (d(x) \cap K(x)) \cup (d(x) \cap \overline{\Phi}) \quad (2.4)$$

Definition 2.3 *A state $x \in X$ is* E-pre-stabilizable *(respectively,* E-stabilizable*) if there exists a state feedback K such that x is E-pre-stable (E-stable) in A_K. The DEDS is* E-stabilizable *if every x is E-stabilizable.* •

We refer the reader to [4] for a complete discussion of this subject and for an $O(n^3)$ test for E-stabilizability, which also constructs a stabilizing feedback.

In [3], we term a system *observable* if the current state is known perfectly at intermittent points in time. Obviously, a necessary condition for observability is that it is not possible for our DEDS to generate arbitrarily long sequences of unobservable events. This is not difficult to check and will be assumed. We now introduce some notation that we will find useful:

- We define the reach of x in A as:

$$R(A, x) = \{y \in X | x \rightarrow^* y\} \quad (2.5)$$

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 1989		**00-09-1989 to 00-09-1989**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Output Stabilizability of Discrete Event Dynamic Systems	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Massachusetts Institute of Technology,Laboratory for Information and Decision Systems,77 Massachusetts Avenue,Cambridge,MA,02139-4307**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**6**	

where $x \rightarrow^* y$ denotes that x reaches y via some event string in Σ^*. We define the reach of x in A as:

$$R(A,x) = \{y \in X | x \rightarrow^* y\} \tag{2.6}$$

- Let Y denote the set of states x such that either there exists an observable transition defined from some state y to x, or x has no transitions defined to it. Let $q = |Y|$.
- Let $L(A,x)$ denote the set of all possible event trajectories of finite length that can be generated if the system is started from the state x. Also, let $L_f(A,x)$ be the set of strings in $L(A,x)$ that have an observable event as the last event, and let $\overline{L}(A) = \bigcup_{x \in X} L(A,x)$.
- Given $s \in L(A,x)$ such that $s = pr$, p is termed a *prefix* of s and we use s/p to denote the corresponding suffix r.

In [3], we describe an observer that computes the subset of Y corresponding to the set of possible states into which A transitioned when the last observable event occurred. Let $Z \subset 2^Y$ denote the observer state space. Then if the observer estimate is $\hat{x}[k] \in Z$ and the next observed event is $\gamma[k+1]$, we have:

$$\hat{x}[k+1] = w(\hat{x}[k], \gamma[k+1]) \tag{2.7}$$

where

$$w(\hat{x}[k], \gamma[k+1]) \triangleq \bigcup_{x \in R(A|\overline{\Gamma}, \hat{x}[k])} f(x, \gamma[k+1]) \tag{2.8}$$

and

$$\gamma[k+1] \in v(\hat{x}[k]) \tag{2.9}$$

where

$$v(\hat{x}[k]) \triangleq h(\bigcup_{x \in R(A|\overline{\Gamma}, \hat{x}[k])} (d(x) \cap u[k]) \cup (d(x) \cap \overline{\Phi})) \tag{2.10}$$

The set Z is then the reach of $\{Y\}$ using these dynamics, i.e., we start the observer in the state corresponding to a complete lack of state knowledge and let it evolve. We let $\hat{\mathbf{x}}(t)$ for $t \in \Gamma^*$ denote the observer state if the string t has been observed. Our observer then is the DEDS $O = (F, w, v, i)$, where $F = (Z, \Gamma, \Gamma, U)$ and i is the identity output function. In [3], we show that A is observable iff O is stable with respect to its singleton states. We also show that if A is observable then all observer trajectories pass through a singleton state in at most q^2 transitions so that the radius of the observer is at most q^3.

Suppose that the observed sequence of transitions includes errors corresponding to inserted, missed, or mistaken events. We term an observer *resilient* if after a finite burst of such measurement errors, the observer resumes correct behavior in a finite number of transitions. The observer O as specified in 2.7,2.9 is defined only for event sequences that can actually occur in the system. When an error occurs, the observer may at some point be in a state such that the next observed event is not defined. In this case, we extend w and v to reset the observer state to $\{Y\}$. This yields an observer $O_R = (F, w_R, v_R, i)$, which is resilient if A is observable.

A compensator is a map $C : \Gamma^* \rightarrow U$, yielding a closed loop system A_C with:

$$\sigma[k+1] \in d_C(x[k], s[k]) \triangleq (d(x[k]) \cap C(h(s[k]))) \cup (d(x) \cap \overline{\Phi}) \tag{2.11}$$

where $s[k] = \sigma[0] \cdots \sigma[k]$ with $\sigma[0] = \epsilon$.

One constraint we wish to place on our compensators is that they preserve liveness. Suppose that we have observed the output string s. Then, we must make sure that any x reachable from any element of $\hat{\mathbf{x}}(s)$ by *unobservable events only* is alive under the control input $C(s)$:

Definition 2.4 *Given $Q \subset X$, $F \subset \Phi$, F is* Q-compatible *if for all $x \in R(A|\overline{\Gamma}, Q)$, $(d(x) \cap F) \cup (d(x) \cap \overline{\Phi}) \neq \emptyset$. A compensator C is* A-compatible *if for all $s \in h(\overline{L}(A))$, $C(s)$ is $\hat{\mathbf{x}}(s)$-compatible.* •

Definition 2.5 *A compensator C is* O-compatible *if for all $s, t \in h(\overline{L}(A))$, such that $\hat{\mathbf{x}}(s) = \hat{\mathbf{x}}(t)$, $C(s) = C(t)$. In this case there exists a map $K : Z \rightarrow U$ such that $C(s) = K(v(\{Y\}, s))$ for $s \in h(\overline{L}(A))$. K is termed the* observer feedback *for C.* •

We will see in Section 3 that we can restrict attention to O-compatible compensators in order to address the stabilization problem.

3 Output Stabilizability

The obvious notion of output E-stabilizability is the existence of a compensator C so that A_C is E-stable. Because of the nature of our observations, it is possible that such a stabilizing compensator may exist, so that we are sure that the state goes through E infinitely often, but so that we never know *when* the state is in E. For this reason, we also define a stronger notion of output stabilizability that requires that we regularly have this information as well. For simplicity, we assume observability throughout.

Definition 3.1 *A is* strongly output stabilizable *if there exists a compensator C and an integer i such that A_C is alive and for all $p \in \overline{L}(A_C)$ such that $|p| \geq i$, there exists a prefix t of p such that $|p/t| \leq i$ and $\hat{\mathbf{x}}(h(t)) \subset E$. We term such a compensator a* strongly output stabilizing *compensator.* •

Proposition 3.2 *A is strongly output stabilizable iff there exists a state feedback $K : Z \rightarrow U$ for the observer such that X_I in $A \parallel O_K$ is E_{OC}-stable, where $X_I = \{(x, \{Y\}) | x \in X\}$ is the set of possible initial states in $A \parallel O_K$ and where $E_{OC} = \{(x, \hat{x}) \in Y \times Z | \hat{x} \subset E\}$ is the set of composite states for which the system is in E and we* know *it.* •

Since O describes all the behavior that can be generated by A, we have the following:

Proposition 3.3 *A is strongly output stabilizable iff there exists a state feedback $K : Z \rightarrow U$ for the observer such that O_K is stable with respect to $E_O = \{\hat{x} \in Z | \hat{x} \subset E\}$ and for all $\hat{x} \in Z$, $K(\hat{x})$ is $\hat{x}$-compatible. Furthermore, if A is strongly output stabilizable then the trajectories in the reach of X_I in $A \parallel O_K$ go through E_{OC} in at most nq^3 transitions.* •

Thus we can test strong output stabilizability by testing the observer for stabilizability. The following algorithm adapts one from [3]:

Proposition 3.4 *The following algorithm tests for strong output stabilizability and constructs the corresponding feedback. It has complexity $O(q^3|Z|)$:*
Algorithm *Let $Z_0 = E_O$ and iterate:*

$$\begin{aligned} P_{k+1} &= \{\hat{x} \in Z | \{\gamma \in v(\hat{x}) | w(\hat{x},\gamma) \in P_k\} \text{ is } \hat{x}\text{-compatible}\} \\ K(\hat{x}) &= \{\gamma \in v(\hat{x}) | w(\hat{x},\gamma) \in P_k\} \text{ for } \hat{x} \in P_{k+1} \\ Z_{k+1} &= Z_k \cup P_{k+1} \end{aligned}$$

Terminate when $Z_{k+1} = Z_k = Z^*$. A is strongly output stabilizable iff $Z = Z^*$. •

Consider next the following somewhat weaker notion:

Definition 3.5 *A is* output stabilizable *(respectively,* output pre-stabilizable*) with respect to E if there exists a compensator C such that A_C is E-stable (E-pre-stable). We term such a compensator an* output stabilizing *(respectively,* output pre-stabilizing*)* compensator. •

Proposition 3.6 *A is output stabilizable iff A is output pre-stabilizable while preserving liveness (i.e., the closed loop system is pre-stable and alive).* •

Our construction of a pre-stabilizing compensator involves (a) constructing a modified observer *which keeps track of the states the system can be in if the trajectory has not yet passed through E*, and (b) formulating the problem of pre-stabilizing A by output feedback as a problem of stabilizing this observer by state feedback.

Consider the following construction: Delete all events in A that originate from the states in E and construct the corresponding observer. Let A_E denote this system and let $O_E = (F_E, w_E, v_E)$ denote its observer. Note that O_E has some "trapping" states, each of which is a subset of E. If the trajectory ever evolves to one of those states, then we know that it has passed through E in A. More generally, for any state $\hat{x}$ of O_E, then for a trajectory that evolves to $\hat{x}$, the system can be in one of the states in $\hat{x} \cap \overline{E}$ only if that trajectory has *not* passed through E yet. By itself O_E does not keep track of enough information to design a pre-stabilizing compensator, since, in order to preserve liveness, we also need to know *all* the states in which the system can be. For this reason we construct $Q = (F_Q, w_Q, v_Q) = O_E \parallel O$ together with the initial state (Y,Y). The state space of Q, is $W = R(Q,(Y,Y))$ which has the same size as that of O_E.

The following lemma shows that the problem of output pre-stabilization can be formulated as a problem of pre-stabilization of Q. The key is to find a state feedback K for Q, which we can then adapt to a corresponding compensator for A, and which forces all trajectories in Q_K to have finite length. In doing this, however, we need to make sure that the compensator for A keeps A alive:

Lemma 3.7 *A is output pre-stabilizable with respect to E while preserving liveness iff there exists a feedback $K : W \to U$ such that for all $(y_1,y_2) \in R(Q_K,(Y,Y))$ $K((y_1,y_2))$ is y_2-compatible, and Q_K is pre-stable with respect to its dead states, i.e., with respect to the states y such that $v_{Q_K}(y) = \emptyset$.* •

In order to construct a compensator as proposed by the above lemma, let us first characterize the states in Q that we can "kill" while preserving liveness in A:

$$E_Q = \begin{array}{l}\{y = (y_1,y_2) \in W | \exists F \subset \Phi \text{ such that} \\ \qquad v_{QF}(y) = \emptyset \text{and } F \text{ is } y_2\text{-compatible}\}\end{array} \tag{3.12}$$

where $v_{QF}(y) = (v_Q(y) \cap F) \cup (v_Q(y) \cap \overline{\Phi})$.

Proposition 3.8 *A is output pre-stabilizable while preserving liveness iff there exists a state feedback K_0 such that Q_{K_0} is E_Q-pre-stable and for all $(y_1,y_2) \in W$, $K((y_1,y_2))$ is y_2-compatible in A. Furthermore, the compensator defined by $C(s) = K(w_{Q_{K_0}}((Y,Y),s))$ for $s \in L(Q_K,(Y,Y))$ and $C(s) = \Phi$ for all other s, pre-stabilizes A, where*

$$K(y = (y_1,y_2)) = \begin{cases} F \subset \Phi | v_{QF}(y) = \emptyset \text{ and} \\ \qquad F \text{ is } y_2\text{-compatible} & \text{if } y \in E_Q \\ K_0(y) & \text{otherwise} \end{cases}$$

Finally, the trajectories in A_C go through E in at most nq^3 transitions. •

Proposition 3.9 *The following algorithm tests for output pre-stabilizability while preserving liveness and constructs the corresponding feedback. It has complexity $O(q^3|W|)$:*
Algorithm *Let $Z_0 = E_Q$ and for $y = (y_1,y_2) \in E_Q$, let $K(y) = F \subset \Phi$ where F is such that $v_{QF}(y) = \emptyset$ and F is y_2-compatible. Iterate:*

$$\begin{aligned} P_{k+1} &= \{y \in W | \{\gamma \in v_Q(y) | w_Q(y,\gamma) \in P_k\} \\ &\qquad \text{is } y_2\text{-compatible in } A\} \\ K(y) &= \{\gamma \in v_Q(y) | w_Q(y,\gamma) \in P_k\} \text{ for } y \in P_{k+1} \\ Z_{k+1} &= Z_k \cup P_{k+1} \end{aligned}$$

Terminate when $Z_{k+1} = Z_k = Z^*$. A is output pre-stabilizable iff $(Y,Y) \in Z^*$. •

Note that if, at some point, we are certain that the trajectory has passed through E, we can force the trajectory to go through E *again* by starting the compensator over, i.e., by ignoring all the observations to date and using the pre-stabilizing compensator on the new observations. We now present an approach which allows us to detect, as soon as possible, that the trajectory has passed though E. Given an output pre-stabilizable A, suppose that C is the corresponding compensator and K is the corresponding Q-feedback for C. Recall that in general, given some $y = (y_1,y_2) \in R(Q_K,(Y,Y))$, not all events defined at y_2 are defined at y. Suppose that we start Q_K in (Y,Y) and then observe $s \in h(\overline{L}(A_C) \cap L(Q_K,(Y,Y)))$, so that $y = w_{Q_K}((Y,Y),s)$ is the present state of Q_K, and suppose that the next observation is a transition $\sigma \notin v_{Q_K}(y)$. We then know that the trajectory has passed through E. At this point, we wish to force the trajectory to pass through E again, but in doing so, we can use our knowledge of the set of states that the system can be in, i.e., $w(y_2,\sigma)$. What we would then like to do is to have Q transition to the state $z = (w(y_2,\sigma), w(y_2,\sigma))$. However, as we have defined it so far, z may *not* be in W. What we must do in this case is to augment W with all such z's and any new subsequent states that might be visited starting from

such a z and using the dynamics of Q (or its restriction under feedback) extended to arbitrary subsets $y_1, y_2 \subset Y$. We modify this definition as follows: if $w_{EK}(y_1, \sigma) = \emptyset$, then we set $w_{Q_K}((y_1, y_2), \sigma)$ to $(w(y_2, \sigma), w(y_2, \sigma))$. Let W^a be the union of the reaches of all states of the form (Y', Y') with $Y' \subset Y$ and define $Q^a = (F^a, w, v)$ where $F^a = (W^a, \Gamma, \Gamma)$. Note that $E_Q \subset W^a$ and $R(Q_K, (Y, Y)) \subset W^a$. If in fact any $z = (Y', Y')$ is pre-stabilizable with respect to $R(Q_K, (Y, Y))$ in Q^a, then we can force the trajectory to pass through E. The next result states that pre-stabilizability of Q is sufficient for being able to do this:

Proposition 3.10 *If there exists a feedback K for Q such that Q_K is E_Q-pre-stable and $K(y)$ is y_2-compatible, then there exists a feedback K' such that for any $Y' \subset Y$, $z = (Y', Y')$ is pre-stable with respect to $R(Q_K, (Y, Y))$ in $Q^a_{K'}$ and $K'(y)$ is y_2-compatible for each $y = (y_1, y_2) \in R(Q^a_{K'}, z)$.* •

Note that K' can be chosen so that $K'(y) = K(y)$ for all $y \in R(Q_K, (Y, Y))$ and the algorithm in Proposition 3.9 can be used for constructing such a K'.

In order to construct an output stabilizing compensator, we use the above proposition recursively as follows: Let K_0 be a feedback that pre-stabilizes Q and preserves liveness, as can be constructed using the algorithm in Proposition 3.9. Let $Z_0 = \{y, y\}$ be the initial state of Q_{K_0} and let $W_0 = R(Q_{K_0}, Z_0)$, i.e., the states we may be in when we know that the trajectory has already passed through E. We then augment Z_0 to include the states to which we may "reset" our compensator:

$$Z_1 = Z_0 \cup \begin{array}{l}\{(\hat{x}, \hat{x}) | \hat{x} = w(y_2, \sigma) \\ \text{for some } y = (y_1, y_2) \in W_0 \text{ and } \sigma \in \hat{v}(y_2, K_0(y))\}\end{array} \quad (3.13)$$

where $\hat{v}(y_2, K_0(y)) = (v(y_2) \cap K_0(y)) \cup (v(y_2) \cap \overline{\Phi})$. Next, we find a feedback K_1 that satisfies Proposition 3.10 for each $(Y', Y') \in Z_1$, and we let $W_1 = R(Q_{K_1}, Z_1)$. Proceeding in this fashion, we construct W_2, W_3, etc., until $W_{k+1} = W_k = W'$ for some k. Let K' be the corresponding feedback. Then (1) $Q_{K'}$ is E_Q-pre-stable; (2) $K'(y)$ is y_2-compatible for all $y \in W'$; and (3) for all $y \in E_Q \cap W'$ and $\sigma \in \hat{v}(y_2, K'(y))$, $(w(y_2, \sigma), w(y_2, \sigma)) \in W'$ Finally, we construct $Q' = (F', w', v')$ where $F' = (W', \Gamma, \Gamma)$:

$$w'(y, \sigma) = \begin{cases} w_Q(y, \sigma) & \text{if } \sigma \in v_{Q_{K'}}(y) \\ (w(y_2, \sigma), w(y_2, \sigma)) & \text{otherwise} \end{cases} \quad (3.14)$$

$$v'(y) = \hat{v}(y_2, K(y)) \quad (3.15)$$

Then, the compensator $C(s) = K'(w'((Y, Y), s))$ for all $s \in L(Q', (Y, Y))$ stabilizes A.

4 Sufficient Conditions Testable in Polynomial Time

We have presented necessary and sufficient conditions for output stabilizability that can be tested in polynomial time in the cardinality of the observer state space. However, while in many cases the observer state space may be small, there are worst cases in which its cardinality is exponential in q (see [3]). In this section, we present sufficient conditions that can always be tested in polynomial time in q.

It is well known in linear system theory that controllability and observability imply stabilizability using dynamic output feedback. Unfortunately, this is not true in our framework, since we only require that the state is known intermittently. We start this section by showing that we obtain a result similar to that for linear systems if we assume as in [5] that after a finite number of transitions, and for each transition after that, we have perfect knowledge of the current state.

A set $Q \subset X$, Q is *f-invariant* in A if all state trajectories from Q stay in Q. In [4], we present an algorithm that computes the maximal f-invariant subset of a given set. Let E_w be the maximal w-invariant subset of the set of singleton states of O. If $E_w \neq \emptyset$ and if O is E_w-stable, then at some finite point the observer state enters E_w and never leave, so that the state will be known perfectly from that point on:

Proposition 4.1 *Suppose that (i) $E \cap E_w = \emptyset$; (ii) A is $E \cap E_w$-stabilizable; (iii) O is E_w-stable, then A is output-stabilizable.* •

To show that the computational complexity of testing Proposition 4.1 is polynomial in q, we proceed as we did in [3]. First, we construct an automaton $A' = (G', f', d', i)$, over Y that models the state transition behavior sampled at the times at which observable events occur so that f' and d' can be constructed from A and i is the identity function). Note that the observers for A and A' are identical. Next, let $P = Y \times Y$ and construct the *pair automaton* O_P with state space P and event set Γ. The dynamics of O_P have the following interpretation. Suppose that the system might be in either state x or state y, and suppose that the event γ occurs. Then, the next state of A' could be any element of $S = f'(x, \gamma) \cup f'(y, \gamma)$ The dynamics of O_P capture this possible ambiguity by moving from (x, y) to *any* (x', y') with $x', y' \in S$. Also, there are some special states in O_P, namely those in $E_P = \{(x, x) | x \in Y\}$, corresponding to no ambiguity. Indeed the following provides an efficient way in which to compute E_w:

Proposition 4.2 *E_w is the maximal w-invariant subset of the singleton states of O iff $\{(x, x) | \{x\} \in E_w\}$ is the maximal w_P-invariant subset of E_P in O_P.* •

Furthermore, it follows from [3] that O is E_w-stable iff O_P is $\{(x, x) | \{x\} \in E_w\}$-stable, and from [4] we can show that Proposition 4.1 can be tested in $O(q^4)$ time.

We can also test a weaker sufficient condition. A set Q is *sustainably (f, u)-invariant* in A if there exists a state feedback such that Q is alive and f-invariant in the closed loop system. Let E_u be the maximal sustainably (w, u)-invariant subset of the singleton states and let K_u be the associated state feedback (see [4] for construction). Note that K_u only needs to act on the singleton states, and thus it can also be thought of as a feedback for A. Note also that K_u needs to disable those events that take states in E_u outside of E_u, and it is unique provided that it *only* disables such events.

Proposition 4.3 *Suppose that (i) $E \cap E_u = \emptyset$; (ii) A is $E \cap E_u$-stabilizable; and (iii) O is E_u-stable. Then if $K_s(x)$ is a stabilizing feedback, the feedback*

$$\hat{K}(\hat{x}) = \begin{cases} K_u(x) \cap K_s(x) & \text{if } \hat{x} = \{x\} \in E_u \\ \Phi & \text{otherwise} \end{cases} \quad (4.16)$$

is an output stabilizing feedback for A. •

It can be shown that this sufficient condition for output stabilizability can also be tested in $O(q^4)$ time.

We conclude this section by presenting an even weaker sufficient condition. We term a state x *always observable* if whenever the system is in x, the observer estimate is $\{x\}$. We term a system *a-observable* if it is stable with respect to its always observable states. Suppose that A is a-observable and let us construct the automaton A_a which is the same as A except that only events in always observable states can be controllable, i.e., $e_a(x) = d(x)$ for all states x that are not always observable. If A_a is stabilizable then A is also output stabilizable since whenever we need to exercise control, we have perfect knowledge of the state:

Proposition 4.4 *Given an a-observable system A, if A_a is E-stabilizable then A is output stabilizable.* •

It can be shown that this sufficient condition can be tested in $O(q^4)$ time.

5 Resiliency

In this section we study the property of resilient output stabilizability in the sense that in spite of a burst of observation errors, the system stays alive and goes through E infinitely often. To begin we say that the discrepancy between two strings s and t is of length at most i, denoted by $\xi(s,t) \leq i$, if there exists a prefix, p, of s and t such that $|s/p| \leq i$ and $|t/p| \leq i$.

Definition 5.1 *A is* resiliently, strongly output stabilizable *if there exists a strongly output stabilizing compensator $C : \Gamma^* \rightarrow U$ and an integer i such that for all strings s that can be generated by A_C, i.e., $\forall x \in X$, and $\forall s \in L_f(A_C, x)$; and for all possible ouput strings t which can be generated by corrupting $h(s)$ with a finite length burst, i.e., $\forall$ positive integers j, and $\forall t \in \Gamma^*$ such that $\xi(t, h(s)) \leq j$, the compensator acting on such corrupted strings still strongly stabilizes the system after the error burst has ended. That is, for each such x, s, and t, the compensator $C'(h(s')) \triangleq C(th(s'))$, defined for $s' \in h(L(A, f(x,s)))$ is such that*

- *the range of $f(x,s)$ is alive in $A_{C'}$, i.e., for all $x \in R(A_{C'}, f(x,s))$, $d_{C'}(x) \neq \emptyset$*
- *for all $p \in L(A_{C'}, f(x,s))$ such that $|p| \geq i$, there exists a prefix p' of p such that $|p/p'| \leq i$ and $f(x,sp) \subset w_{CR}(\{Y\}, th(p')) \subset E$, where w_{CR} is the transition function of the resilient observer O_{CR} for A_C.*

We say that C is a resiliently, strongly stabilizing compensator *for A.* •

The requirements on C' ensure that the compensator C acting on the corrupted output string (a) preserves liveness, and (b) stabilizes A following the burst.

Let us return to the characterization of strong output stabilizability in Proposition 3.3, but note that we must now use the resilient observer O_R in place of O in the actual implementation. If an error burst now occurs, it may put the system and observer in arbitrary states not necessarily within the reach of the initial states X_I defined in Proposition 3.3. Since $A \parallel O_{KR} = A \parallel O_K$, we have:

Proposition 5.2 *A is resiliently, strongly output stabilizable if there exists a state feedback $K : Z \rightarrow U$ for the observer such that $A \parallel O_K$ is E_{OC}-stable.* •

Finally, we have the following companion of Proposition 3.2 which states that it is necessary and sufficient to test O for E_O-stability, but since the burst may put the system and the observer in arbitrary states, we need an X-compatible feedback:

Proposition 5.3 *A is resiliently, strongly output stabilizable with respect to E iff there exists a state feedback K for the observer such that O_K is E_O-stable and for all $\hat{x} \in Z$, $K(\hat{x})$ is X-compatible.* •

An algorithm for testing resilient, strong output stabilizability and constructing a feedback is identical to Algorithm 3.4 except that when we search for a feedback, we search for one that is X-compatible, and the computational complexity is again $O(q^3|Z|)$.

Definition 5.4 *A is* resiliently output stabilizable *if there exists an output stabilizing compensator C such that for all strings s that can be generated by A_C, i.e., $\forall x \in X$, and $\forall s \in L_f(A_C, x)$; and for all possible ouput strings t which can be generated by corrupting $h(s)$ with a finite length burst, i.e., $\forall$ positive integers i, and $\forall t \in \Gamma^*$ such that $\xi(t, h(s)) \leq i$, the trajectories starting from $f(x,s)$ visit E infinitely often, i.e., $f(x,s)$ is E-stable in $A_{C'}$, where $C'(h(s')) = C(th(s'))$ for all $s' \in h(L(A, f(x,s)))$. We say that C is a* resiliently stabilizing compensator *for A.* •

Lemma 5.5 *If C is a resilient output stabilizing compensator then $C(s)$ is X-compatible for all $s \in h(\overline{L}(A))$.* •

Necessary and sufficient conditions for resilient output stabilizability parallel those of output stabilizability except that we need to use X-compatible feedback. Since, a resilient output stabilizing compensator needs to be defined for all strings in Γ^*, given a feedback K for the automaton Q defined in Section 3.2, we define $Q_{KR} = (G_{KR}, w_{KR}, v_{KR})$ so that $v_{KR}(\Gamma) = (\Gamma)$ and $w_{K,R}(y, \gamma)$ resets Q_K to (Y,Y) if $\gamma \notin v_{Q_K}(y)$ We can then define a compensator $C(s) = K(w_{KR}((Y,Y), s))$ for all $s \in \Gamma^*$. We state the following companion of Proposition 3.8 where

$$E_{QR} = \begin{array}{l}\{y = (y_1, y_2) \in W | \exists F \subset \Phi \text{ such that} \\ \quad v_{QF}(y) = \emptyset \text{ and } F \text{ is } X\text{-compatible}\}\end{array} \quad (5.17)$$

Proposition 5.6 *A is resiliently ouput stabilizable iff there exists a state feedback K such that Q_K is E_{QR}-pre-stable and for all $y \in W$, $K(y)$ is X-compatible in A. Furthermore, the compensator defined by $C(s) = K(w_{KR}((Y,Y), s))$ for all $s \in \Gamma^*$ resiliently stabilizes A.* •

We can test for resilient output stabilizability and can construct a feedback by modifying Algorithm 3.4, using E_{QR} in place of E_Q and checking X-compatibility.

Acknowledgements

Research supported by the Air Force Office of Scientific Research under Grant AFOSR-88-0032 and by the Army Research Office under Grant DAAL03-86-K0171.

References

[1] R. Cieslak, C. Desclaux, A. Fawaz, and P. Variaya. Modeling and control of discrete event systems. In *Proceedings of CDC*, December 1986.

[2] J. S. Ostroff and W. M. Wonham. A temporal logic approach to real time control. In *Proceedings of CDC*, December 1985.

[3] C. M. Özveren and A. S. Willsky. Observability of discrete event dynamic systems. Submitted to the *IEEE Transactions on Automatic Control.*

[4] C. M. Özveren, A. S. Willsky, and P. J. Antsaklis. Stability and stabilizability of discrete event dynamic systems. Submitted to the *Journal of the ACM.*

[5] C. M. Özveren. Analysis and control of discrete event dynamic systems: A state space approach. *PhD Thesis, MIT*, August 1989.

[6] P. J. Ramadge. Observability of discrete event systems. In *Proceedings of CDC*, December 1986.

[7] P. J. Ramadge and W. M. Wonham. Modular feedback logic for discrete event systems. *SIAM J. of Cont. and Opt.*, September 1987.

[8] P. J. Ramadge and W. M. Wonham. Supervisory control of a class of discrete event processes. *SIAM J. of Cont. and Opt.*, January 1987.

[9] J. N. Tsitsiklis. On the control of discrete event dynamical systems. In *Proceedings of CDC*, December 1987.

[10] A. F. Vaz and W. M. Wonham. On supervisor reduction in discrete event systems. *International Journal of Control*, 1986.